UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,504	01/27/2004	Kouhei Nadehara	Q79582	9262

23373 7590 12/16/2009
SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
MORAN, RANDAL D	
ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
12/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sughrue@sughrue.com
PPROCESSING@SUGHRUE.COM
USPTO@SUGHRUE.COM

Office Action Summary	**Application No.** 10/764,504	**Applicant(s)** NADEHARA, KOUHEI	
	Examiner RANDAL D. MORAN	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

Claims 1-20 are pending.

This action is in response to the communication filed 1/16/2009.

Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. **Claims 1-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Van Buer (20030198345)**, hereafter "Van Buer", in view of **Takagi et al. (US 6,259,790)**, hereafter "Takagi".

As per **claim 1, 3, 6, 8, and 15-20**, Van Buer discloses: a selector unit selecting an element of a state in response to row and column indices (0007);
a S-box for obtaining a substitution value with said selected element used as an index (0063); first to fourth Galois field multiplexers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively, the first and fourth products corresponding to a same one column of the state (0054, 0055, 0058, 0063-0064); and
an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state (0067-0070).
Van Buer does not explicitly disclose a coefficient table providing first to fourth coefficients in response to said row index.
Takagi discloses a coefficient table providing first to fourth coefficients in response to said row index (Fig. 13, column 26, lines 54-67, column 27, lines 1-5).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Van Buer by a coefficient table providing first to fourth coefficients in response to said row index as taught by Takagi to provide a solution to the problem that the security and the speed are not compatible with each other because a higher security level requires a larger key size but a larger key size but a larger key size implies a lower encryption/decryption speed (Takagi-column 6- lines 27-31).

As per **claim 11, 12 and 14**, the combination discloses a first selector unit selecting an element of a state in response to row and column indices (0007);

an inverse affine transformation circuit applying an inverse affine transformation on said selected element (0059-0063);

a second selector unit selecting one out of two data bytes consisting of said selected element received from said first selector, and a result of said inverse affine transformation received said inverse affine transformation circuit, wherein said selected element is selected for encryption, while said result of said inverse affine transformation is selected for decryption (Fig. 25);

an inverse determining unit obtaining a multiplicative inverse of said selected data byte received from said second selector (Fig. 25);

an affine transformation circuit applying 20 an affine transformation on said obtained multiplicative inverse (0063);

a third selector unit selecting one of two data bytes consisting of said multiplicative inverse received from said inverse determining unit, and a result of said affine transformation received from affine transformation circuit, wherein said result of said affine transformation is selected for decryption, while said multiplicative inverse is selected for encryption (0066-0067);

a coefficient table providing first to fourth coefficients in response to said row index;

first to fourth Galois field multiplexers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients (Takagi- Fig. 13, column 26, lines 54-67, column 27, lines 1-5), respectively, and an accumulator which accumulates the first to fourth products to develop first to fourth elements of a designated column of a resultant state (0054, 0055, 0058, 0063-0064).

As per **claim 2, 5, 7, and 10**, the combination discloses: wherein said first to fourth coefficients are respectively set to {02}, (01}, {01}, and {03} in response to said row index selecting a first row of said state, to {03}, {02}, (01}, and (01} in response to said row index selecting a second row of said state, to (01}, (03}, (02}, and (01} in response to said row index selecting a third row of said state, and to {01}, {01), {03}, and {02) in response to said row index selecting a fourth row of said state (0070-0075).

As per **claims 4, 9 and 13**, the combination discloses: a processing unit adapted to implement XORing, wherein said AES encryption processor is further adapted to an XOR instruction, and wherein said processing unit implements XORing of values contained in two selected registers of said register file (0060).

Response to Arguments

Applicant's arguments filed 7/27/2009 have been fully considered but they are not persuasive.

Regarding **Claims 1,** applicant's arguments have been fully considered but are not persuasive. With respect to applicant's argument that the combination fails to teach *a coefficient table providing first to fourth coefficients in response to said row index*, applicant is directed to Takagi - column 26- lines 54-67, column 27- lines 1-5.In response to applicant's argument that the reference uses RSA encryption as opposed to AES encryption, a recitation of the intended use (i.e. using AES encryption) of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. The actual encryption used does not distinguish the claims from the prior art as the prior teaches a coefficient table as recited in the claims.

With respect to applicant's argument that the combination fails to teach first to fourth field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively, applicant is directed to Van Buer – [0063][0064]. Van Buer discloses "The output of the exclusive-or circuit 114 of FIG. 2 can be a data block of the same width as was in block 110, which can form an input 120 to a substitution circuit 122, as shown in more detail in FIG. 3. The input data block can be treated as a series of 8-bit octets A, B, C . . . to P in the case of 128 bits, i.e., 16 octets, A, B, C . . . XH, in the case of 192 bits, i.e., 24 octets and A, B, C . . . XP in the case of 256 bits, i.e., 32 octets. Each octet can be used as an index into a substitution table (or inverse table during decryption), and the output into data block 124 can be the octet value in the table within the respective S-Box, e.g., S1 . . . S16, i.e., the A, B, C . . . P in the substitution stage data block 124. Such a look-up table is referred to herein as an S-Box S1, S2, S3 . . . S16 or S24 or S32. Because the octets are independent in this step, maximum speed can be achieved by providing, e.g., 32 copies of the respective S-Boxes, S1 . . . S32, for 256-bit Rijndael data blocks, or, e.g., 16 copies of the table S1 . . . S16, for 128-bit AES, which can be implemented, e.g., as a read-only memory, and processing the entire block 120 in parallel, as illustrated in FIG. 3.

This substitution step can have the highest gate complexity in an implementation according to the present invention, since each table could contain 256 octets of data, 2048 bits in all. In applications where speed is less important, overall complexity could be reduced by implementing fewer copies of the tables, adding multiplexers and latches and using multiple clock cycles to perform substitution over different parts of the data block 120 in turn in each round." Van Buer discloses the output of the x-or circuit can form inputs into the substitution circuit and can be treated as a series of various octets. In response to applicant's argument that the combination doesn't explicitly teach the 1st to 4th coefficients, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/R. D. M./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435